(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－31129

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ａ
	13/00	３５１		13/00	３５１Ｅ
	17/30			15/40	３１０Ｆ
Ｈ０４Ｌ	9/32				３２０Ｂ
			Ｈ０４Ｌ	9/00	６７３Ｃ

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－188524

(22)出願日　平成９年(1997)７月14日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　中島　充
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　門間　仁
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

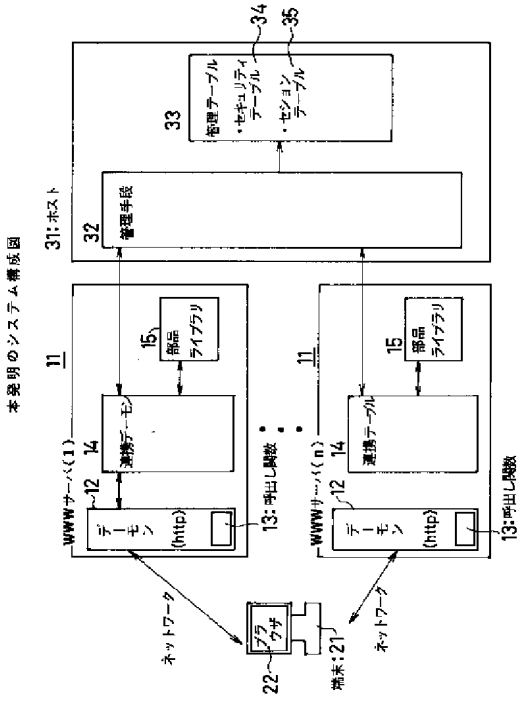
(74)代理人　弁理士　岡田　守弘

(54)【発明の名称】　複数WWWサーバ連携システム

(57)【要約】

【課題】　本発明は、複数ＷＷＷサーバ連携システムに関し、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセションＩＤをもとに複数ページや異なる複数のＷＷＷサーバに渡ってアクセスを可能にするシステムを実現することを目的とする。

【解決手段】　ホストは複数のいずれかのＷＷＷサーバから通知されたブラウザからのＨＴＭＬ文書を解析し、セションＩＤが付加されていなかったときにユーザ情報の入力要求を上記ＷＷＷサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセションＩＤを生成し、ふたたびＷＷＷサーバを介してセションＩＤの埋め込んだＨＴＭＬ文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すように構成する。



1

【特許請求の範囲】

【請求項１】ブラウザから受信したＨＴＭＬ文書をホストに通知、およびホストから通知を受けたセションＩＤをＨＴＭＬ文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をブラウザに送信する複数のＷＷＷサーバ等を備えたネットワークシステムにおいて、

上記ホストは上記複数のいずれかのＷＷＷサーバから通知されたブラウザからのＨＴＭＬ文書を解析し、セションＩＤが付加されていなかったときにユーザ情報の入力要求を上記ＷＷＷサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセションＩＤを生成し、ふたたびＷＷＷサーバを介してセションＩＤの埋め込んだＨＴＭＬ文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すことを特徴とする複数ＷＷＷサーバ連携システム。

【請求項２】上記セションＩＤをＨＴＭＬ文書に埋め込む際に、ＵＲＬ上に表示しないようにセションＩＤをＨＴＭＬ文書上に埋め込み、セションＩＤを不可視としたことを特徴とする請求項１記載の複数ＷＷＷサーバ連携システム。

【請求項３】上記ＷＷＷサーバに、

ブラウザとの間でＨＴＭＬ文書の送受信を行うデーモン中に連携デーモンを呼び出す呼び出し関数と、

この呼び出し関数から呼び出されたときにブラウザから受信したＨＴＭＬ文書をホストに通知、およびホストから通知を受けたセションＩＤをＨＴＭＬ文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をブラウザに送信する連携デーモンとを備えたことを特徴とする請求項１あるいは請求項２記載の複数ＷＷＷサーバ連携システム。

【請求項４】上記ＷＷＷサーバに、

上記連携デーモンから依頼を受けた処理を実行するる部品ライブラリを備えたことを特徴とする請求項３記載の複数ＷＷＷサーバ連携システム。

【請求項５】上記有効時間情報として、上記ユーザ情報に対応づけて認証有効時間を設定したことを特徴とする請求項１ないし請求項４記載のいずれかの複数ＷＷＷサーバ連携システム。

【請求項６】上記ＷＷＷサーバ上のＨＴＭＬ文書毎あるいは複数のＨＴＭＬ文書をまとめたディレクトリ毎に認証の有無を設定し、認証有のときにのみ上記呼び出し関数が上記連携デーモンを呼び出すことを特徴とする請求項３ないし請求項５記載のいずれかの複数ＷＷＷサーバ連携システム。

【請求項７】ブラウザから受信したＨＴＭＬ文書をホストに通知、およびホストから通知を受けたセションＩＤをＨＴＭＬ文書に埋め込んでブラウザに送信あるいはホストから通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をブラウザに送信するＷＷＷサーバ上で動作するプログラムを格納した記録媒体。

2

【請求項８】複数のいずれかのＷＷＷサーバから通知されたブラウザからのＨＴＭＬ文書を解析し、セションＩＤが付加されていなかったときにユーザ情報の入力要求をＷＷＷサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセションＩＤを生成し、ふたたびＷＷＷサーバを介してセションＩＤの埋め込んだＨＴＭＬ文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すホスト上で動作するプログラムを格納した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数ＷＷＷサーバが連携する複数ＷＷＷサーバ連携システムに関するものである。

【０００２】

【従来の技術】従来、ＷＷＷサーバの通信プロトコルであるＨＴＴＰ(Hyper Text Transfer Protocol)のセションは、ブラウザがページを要求するときに設定し、サーバがそのページを送信すると切断されてしまう。このようにセションは、ページごとに切れてしまい、次のページ（画面）にアクセスした場合には、全く別のセションになる。

【０００３】そのため、利用者の認証が必要なページに対しては、ページ単位に利用者の認証を行うようにしていた。

【０００４】

【発明が解決しようとする課題】上述したように従来の認証は、ブラウザからＷＷＷサーバのページをアクセスする毎に利用者認証を要求し、ブラウザがその認証に必要な情報（ユーザＩＤ、パスワードなどの情報）を入力して送信しサーバが認証を行うという面倒な操作が認証な必要なページ毎に発生してしまうという問題があった。

【０００５】また、ブラウザから同一機能の他のＷＷＷサーバをアクセスした場合には、当然に認証が必要なページ毎にその認証に必要な情報を入力して送信しサーバが認証を行わなければならないという問題もあった。

【０００６】本発明は、これらの問題を解決するため、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセションＩＤをもとに複数ページや異なる複数のＷＷＷサーバに渡ってアクセスを可能にするシステムを実現することを目的としている。

【０００７】

【課題を解決するための手段】図１を参照して課題を解決するための手段を説明する。図１において、ＷＷＷサーバ１１は、ブラウザ２２から受信したＨＴＭＬ文書をホスト３１に通知したり、ホスト３１から通知を受けた

セションＩＤをＨＴＭＬ文書に埋め込んでブラウザ２２に送信あるいはホスト３１から通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をブラウザ２２に送信したりなどするものであって、デーモン１２、連携デーモン１４、部品ライブラリ１５などから構成されるものである。

【０００８】デーモン１２は、データをブラウザ２２との間でネットワークを介して送受信するものであって、ここでは、呼び出し関数１３などを持つものである。呼び出し関数１３は、ブラウザ２２からＨＴＭＬ文書を受信したときに連携デーモン１４を呼び出すものである。

【０００９】連携デーモン１４は、呼び出し関数１３から呼び出され、デーモン１２が受信したＨＴＭＬ文書をホスト２１に通知したり、ホスト３１から通知されたＨＴＭＬ文書をデーモン１２に通知したり、部品ライブライ１４を呼び出して所定処理を依頼したりなどするものである。

【００１０】部品ライブラリ１５は、連携デーモン１４から依頼を受けた各種処理を行う部品（プログラム）である。ブラウザ２２は、ネットワークを介してＷＷＷサーバ１１と接続して当該ＷＷＷサーバ１１から受信したＨＴＭＬ文書を画面に表示したり、画面上で文書／イメージが選択されたときに該当するＨＴＭＬ文書などをＷＷＷサーバ１１に送信したりなどするものである。

【００１１】ホスト３１は、ＷＷＷサーバ１１を構成する連携デーモン１４から通知されたＨＴＭＬ文書をもとに各種処理を行ったり、データを連携デーモン１４経由でブラウザ２２に送信したりなどするものである。

【００１２】次に、動作を説明する。ＷＷＷサーバ１１がブラウザ２２から受信したＨＴＭＬ文書をホスト３１に通知し、ホスト３１が通知されたブラウザ２２からのＨＴＭＬ文書を解析し、セションＩＤが付加されていなかったときにユーザ情報の入力要求をＷＷＷサーバ１１を介してブラウザ２２に送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセションＩＤを生成し、ふたたびＷＷＷサーバ１１を介してセションＩＤの埋め込んだＨＴＭＬ文書をブラウザ２２に送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許すようにしている。

【００１３】この際、セションＩＤをＨＴＭＬ文書に埋め込むときに、ＵＲＬ上に表示しないようにセションＩＤをＨＴＭＬ文書に埋め込み、セションＩＤを不可視とするようにしている。

【００１４】また、ＷＷＷサーバ１１に、ブラウザ２２との間でＨＴＭＬ文書などの送受信を行うデーモン１２中に連携デーモン１４を呼び出す呼び出し関数１３を設け、呼び出し関数１３から呼び出された連携デーモン１４がブラウザ２２から受信したＨＴＭＬ文書をホスト３１に通知し、ホスト３１から通知を受けたセションＩＤをＨＴＭＬ文書に埋め込んでデーモン１２を介してモブ

ラウザ２２に送信あるいはホスト３１から通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をデーモン１２を介してブラウザ２２に送信するようにしている。

【００１５】また、ＷＷＷサーバ１１に、連携デーモン１４から依頼を受けた処理を実行するる部品ライブラリ１５を設け、当該部品ライブラリ１５に各種処理を依頼するようにしている。

【００１６】また、ホスト３１が有効時間情報として、ユーザ情報に対応づけて認証有効時間を設定し、セションＩＤの有効性を判断するようにしている。また、ＷＷＷサーバ１１上のＨＴＭＬ文書毎に認証の有無を設定し、認証有のときにのみ呼び出し関数１３が連携デーモン１４を呼び出すようにしている。

【００１７】従って、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセションＩＤをもとに複数ページや異なる複数のＷＷＷサーバ１１に渡ってアクセスすることが可能となる。

【００１８】

【発明の実施の形態】次に、図１から図８を用いて本発明の実施の形態および動作を順次詳細に説明する。

【００１９】図１は、本発明のシステム構成図を示す。図１において、ＷＷＷサーバ１１は、ブラウザ２２からネットワークを介して受信したＨＴＭＬ文書をホスト３１に通知したり、ホスト３１から通知を受けたセションＩＤをＨＴＭＬ文書に埋め込んでネットワークを介してブラウザ２２に送信あるいはホスト３１から通知を受けたセションＩＤを埋め込んだＨＴＭＬ文書をネットワークを介してブラウザ２２に送信したりなどするものであって、デーモン１２、連携デーモン１４、部品ライブラリ１５などから構成されるものである。このＷＷＷサーバ１１は、例えば後述する図２中のＷＷＷサーバと記載した処理を行う。ここで、ＨＴＭＬ文書はブラウザの画面上に文書やイメージを表示するようにＨＴＭＬ言語で記述した文書であり、他にＵＲＬ（アドレス）およびヘッダ情報（ＨＴＴＰプロトコルで使用する情報）がある。

【００２０】デーモン（ｈｔｔｐ）１２は、ＨＴＴＰプロトコルを使用してネットワークを介してデータ（ＵＲＬ、ｈｔｍｌＬ文書など）をブラウザ２２との間で授受するものであって、ここでは、呼び出し関数１３などを持つものである。

【００２１】呼び出し関数１３は、ブラウザ２２からＨＴＭＬ文書を受信したときに連携デーモン１４を呼び出すものである。連携デーモン１４は、呼び出し関数１３から呼び出され、デーモン１２が受信したＨＴＭＬ文書をホスト２１に通知したり、ホスト３１から通知されたＨＴＭＬ文書をデーモン１２に通知したり、部品ライブライ１４を呼び出して所定処理を依頼したりなどするものであって、例えば後述する図２中に連携デーモンと記載した処理を行うものである。

5

【００２２】部品ライブラリ１５は、連携デーモン１４から依頼を受けた各種処理を行う部品であって、例えば後述する図２中に部品と記載した処理を行うものである。端末２１は、ネットワークを介してWWWサーバ１１と接続し、ＨＴＴＰプロトコルを用いてデータの授受を行うものであって、ここでは、ブラウザ２２などから構成されるものである。

【００２３】ブラウザ２２は、ネットワークを介してWWWサーバ１１と接続して当該WWWサーバ１１から受信したＨＴＭＬ文書を画面に表示したり、画面上で文書／イメージが選択されたときに該当するＨＴＭＬ文書などをWWWサーバ１１に送信したりなどするものであって、ネットエスケープ（製品名）などの汎用のブラウザ（ＨＴＭＬ文書を表示などするプログラム）である。

【００２４】ホスト３１は、WWWサーバ１１を構成する連携デーモン１４から通知されたＨＴＭＬ文書をもとに各種処理を行ったり、データを連携デーモン１４経由でブラウザ２２に送信したりなどするものであって、ここでは、管理手段３２および管理テーブル３３などから構成されるものであり、後述する図２のホストと記載した各種処理を行うものである。

【００２５】管理手段３１は、管理テーブル３２を参照して認証を行ったり、認証ＯＫのときにデータをブラウザ２２に向けて送信したりなどするものである。管理テーブル３２は、各種管理情報を登録して管理するテーブルであって、ここでは、セキュリティテーブル３４およびセションテーブル３５などから構成されるものである。

【００２６】セキュリティテーブル３４は、ＨＴＭＬ文書のセキュリティ情報を管理するものであって、例えば後述する図３に示すような情報を管理するものである。セションテーブル３５は、セションＩＤの認証有効時間を管理するものであって、ここでは、例えば後述する図４に示すような情報を管理するものである。

【００２７】次に、図２に示す順番に従い、図１の構成の動作を詳細に説明する。図２は、本発明の動作説明図を示す。ここで、ブラウザ、WWWサーバ、およびホストは、図１のブラウザ２２、WWWサーバ１１、およびホスト３１にそれぞれ対応するものである。

【００２８】図２において、Ｓ１は、参照するＵＲＬの指定を行う。これは、ブラウザ２２が参照するＵＲＬ（アドレス）の指定に対応して、当該ＵＲＬをWWWサーバ１１に送信する。

【００２９】Ｓ２は、WWWサーバ１１がＵＲＬを受け取る（受信する）。Ｓ３は、ＵＲＬの解析を行う。Ｓ４は、Ｓ３のＵＲＬの解析の結果、プラグイン関数の呼び出しか判別する。ＹＥＳの場合には、本発明に係る以下の処理を実行し、Ｓ７で呼び出し関数１３が連携デーモン１４を呼び出し、Ｓ８で常駐デーモン（連携デーモン）への引渡を行い、Ｓ９で認証要求をホスト３１に通知し、Ｓ１０に進む。一方、Ｓ４のＮＯの場合には、プラグイン関数の呼出しがないと判明したので、Ｓ５でｈｔｍｌ文書の送出を行い、Ｓ８でブラウザ２２がｈｔｍｌ文書を画面上に表示する。

6

【００３０】以上のＳ１ないしＳ９によって、ブラウザ２２が参照するＵＲＬをWWWサーバ１１に送信し、WWWサーバ１１のデーモン（ｈｔｔｐ）１２がＵＲＬを受信してプラグイン関数呼出しが必要か否かを判別し、ＹＥＳの場合（必要な場合）には連携デーモン１４を呼出し、認証要求をホスト３１に通知することが可能となり、一方、ＮＯの場合（必要でない場合）には従来通り、ＵＲＬに対応するｈｔｍｌ文書をブラウザ２２に送信してブラウザ２２がｈｔｍｌ文書を画面上に表示することが可能となる。

【００３１】Ｓ１０は、ホスト３１が連携デーモン１４からの認証要求を受け取る。Ｓ１１は、ＵＲＬの解析を行う。Ｓ１２は、認証が必要なＵＲＬかどうかの判定を行う。これは、ＵＲＬで指定されたｈｔｍｌ文書が認証を必要とするものであるか否かについて、後述する図２のセキュリティテーブル３４を参照して判定する。認証が必要な場合には、Ｓ１５に進む。一方、認証が不要の場合には、Ｓ１３でｈｔｍｌ文書をWWWサーバ１１を介してブラウザ２２に送信し、Ｓ１４でブラウザ２２が受信したｈｔｍｌ文書について画面上に表示する。

【００３２】Ｓ１５は、Ｓ１２で認証が必要と判明したので、指定されたＵＲＬの認証範囲の取り出しを行う。Ｓ１６は、セションＩＤが付加されているか判別する。これは、Ｓ１５でブラウザ２２から受信したＵＲＬの認証範囲にセションＩＤが付加されているか判別する（既に以前にセションＩＤが付加されているか判別する）。ＹＥＳの場合には、既に以前にセションＩＤがＳ１７ないし３７によってセットされていたと判明したので、Ｓ４１に進む。一方、ＮＯの場合には、セションＩＤがセット（付加）されていないと判明したので、Ｓ１７ないしＳ３２によってセションＩＤの付加を行う。

【００３３】Ｓ１７は、Ｓ１６でセションＩＤが付加されていないと判明したので、ＩＤ、パスワード画面（ｊａｖａ）の送出要求をWWWサーバ１１に通知する。Ｓ１８は、WWWサーバ１１の連携デーモン１４が受け付ける。

【００３４】Ｓ１９は、Ｓ１８で受け付けた連携デーモン１４から部品ライブラリ１５中の部品がＩＤ、パスワード入力用ｈｔｍｌ（ｊａｖａ、ｈｔｍｌ）を送出する。Ｓ２０は、Ｓ１９で送出されたパスワード入力用ｈｔｍｌ（ｊａｖａ）の表示をブラウザ２２上で行う。

【００３５】Ｓ２１は、Ｓ２０で表示されたパスワード入力用画面上でＩＤ、パスワード入力する。例えば後述する図５のパスワード／ＩＤ入力画面上でユーザがユーザＩＤ、パスワードを入力し、ＳＴＡＲＴボタンを押下する。

【００３６】Ｓ２２は、ＩＤ、パスワードを暗号化（ｊａｖａ）してＷＷＷサーバ１１に送信する。Ｓ２３は、受取情報の送出（再暗号化）を行う。これは、ＷＷＷサーバ１１がＳ２２で送信されたＩＤ、パスワードの暗号化した情報を受け取り、この情報を再暗号化してホスト１１に送信する。

【００３７】Ｓ２４は、ホスト３１がＳ２３で送信された情報を受け取し、復号化する。Ｓ２５は、Ｓ２４で復号化したＩＤ、パスワードを取り出す。Ｓ２６は、ＩＤ、パスワードの検索を行う。これは、例えば後述する図４のセションテーブル３５中のＩＤ（ユーザＩＤ、パスワード）の検索を行い、一致するものがあるか判別する。ＯＫの場合には、Ｓ２９に進む。ＮＧの場合には、一致するＩＤ、パスワードが登録されていないくエラーと判明したので、ＷＷＷサーバ１１に指示してＳ２７でエラー表示用ｈｔｍｌを送信し、Ｓ２８でブラウザ２２が受信したエラー表示ｈｔｍｌによって画面上にエラー表示を行う。

【００３８】Ｓ２９は、Ｓ２６でＩＤ、パスワードを検索して一致するものがあると判明したので、更に認証範囲の判定を行う。これは、図示外のユーザＩＤ毎の認証範囲の判定を行い、当該ユーザＩＤに認証権限を付与されているか判別する。ＯＫの場合には、Ｓ３０に進む。ＮＧの場合には、ユーザＩＤに認証権限が付与されていないと判明したので、Ｓ２７でエラー表示用ｈｔｍｌを送出し、Ｓ２８でブラウザ２２がエラー表示ｈｔｍｌを画面上に表示する。

【００３９】Ｓ３０は、Ｓ２９のＯＫで認証権限がありと判明したので、セションＩＤのセットを行う。セションＩＤは、一意のＩＤであって、例えば後述する図４に示すように、現時刻の年月日時分秒ミリ秒からなる一意のセションＩＤを、図４のセションテーブル３５中のセションＩＤの該当する欄にセットして記憶する。

【００４０】Ｓ３１は、認証保証時間のセットを行う。これは、後述する図４のセションテーブル３５の認証有効時間を取り出して現時刻に加算して認証満了時間を求めて図４の当該認証満了時間の欄にセットする。

【００４１】Ｓ３２は、セションＩＤの送出を行う。Ｓ３３は、ＷＷＷサーバ１１の連携デーモン１４がＳ３２で送出されたセションＩＤを受け取る。

【００４２】Ｓ３４は、部品が指定されたＵＲＬにセションＩＤを付加する。これは、例えば後述する図８の（ａ）の指定されたＵＲＬにセションＩＤを付加し、図８の（ｂ）のＵＲＬ（セションＩＤ付加）を生成する。

【００４３】Ｓ３５は、付加ＵＲＬを固定のＵＲＬに再編集する。これは、Ｓ３４でセションＩＤを付加した図８の（ｂ）のＵＲＬ（セションＩＤ付加）について、固定のＵＲＬとして、図８の（ｃ）のＵＲＬ（ｃｇｉ付加）を生成、即ち、システムで固定のデータを図示のように付加し、元の正しいセションＩＤをｈｔｍｌ文書中に埋め込み、ＵＲＬ（ｃｇｉ付加）が明示的に表示されてもセンションＩＤが表示されないようにして他人に見えないようにする（不可視にする）。

【００４４】Ｓ３６は、ｈｔｍｌ文書を送出する。Ｓ３７は、Ｓ３６で送出されたｈｔｍｌ文書をブラウザ２２が画面上に表示する。この際、ＵＲＬ（ｃｇｉ）が表示されるが、当該ＵＲＬにはシステムで固定のｃｇｉ（例えば××××．ｃｇｉ）が表示されるのみで、正しいセションＩＤは不可視とし、ｈｔｍｌ文書中に埋め込むようにしている。そして、Ｓ１に戻り繰り返す。

【００４５】また、Ｓ４１は、Ｓ１６でセションＩＤが付加されていると判明したので、セションＩＤの検索を行う。これは、セションＩＤについて、図４のセションテーブル３５に登録されているか判別する。ＯＫの場合には、Ｓ４２に進む。ＮＧの場合には、セションＩＤがセションテーブル３５に登録されていないと判明したので、既述したＳ１７以降の処理を行い、セションＩＤの再登録を行う。

【００４６】Ｓ４２は、セションＩＤの有効範囲内か判別する。これは、後述する図４のセションテーブル３５を参照して該当するセションＩＤのエントリ中の認証満了時間内に、現時刻があって当該セションＩＤが有効か判別する。ＯＫの場合には、既述したＳ３３以降の処理を実行する。ＮＧの場合には、セションＩＤがセションテーブル３５に登録されているが有効時間範囲内でないと判明したので、既述したＳ１７以降の処理を行い、セションＩＤの再登録を行う。

【００４７】以上によって、ＵＲＬ解析を行い、認証が必要なＵＲＬの場合には、セションＩＤが付加されていないときにＩＤ、パスワード入力画面をブラウザ２２に送信して表示させ、入力されたＩＤ、パスワードが正しいときに一意のセションＩＤを付加し、一方、セションＩＤが付加されていたときに当該セションＩＤが有効時間範囲内のときにセションＩＤをｈｔｍｌ文書中に不可視に付加してブラウザ２２に送信し、また、セションＩＤが付加されていても有効時間範囲内でないときはＩＤ、パスワード入力画面をブラウザ２２に送信して表示させ、入力されたＩＤ、パスワードが正しいときに一意のセションＩＤを再付加することにより、ｈｔｍｌ文書中に不可視に埋め込んだセションＩＤをもとに、有効時間範囲内についてブラウザ２２とホスト３１とが任意のＷＷＷサーバ１１を経由して送受信することが可能となる。以下順次詳細に説明する。

【００４８】図３は、本発明のセキュリティテーブル例を示す。これは、ＳＯＰ、ＴＹＰＥ、ＵＲＬを対応づけて登録したものである。ここで、ＳＯＰは、図示のように

・００１：サビービス種別を表し
・ＰＵＢ：公開を表し
・ＢＡＳ：基本を表す。

【００４９】また、ＴＹＰＥは、図示のように
・００：認証（有料）を表す。
・０１：認証（無料）を表す。
【００５０】
・ＢＳ：基本を表す。
・ＰＵＢ：公開を表す。
また、ＵＲＬは図示のようにディレクトリ、ｈｔｍｌ文書をつなげたものである。
【００５１】以上のように、セキュリティテーブル３４によって、ｈｔｍｌ文書毎にＳＯＰ、ＴＹＰＥできまるセキュリティを登録して管理するようにしたものである。図４は、本発明のセションテーブル例を示す。このセションテーブル３５は、図示のように、ユーザＩＤ、パスワードに対応づけて認証有効時間、パトロール時間、タイマ監視時間を予め登録しておき、実際にブラウザ２２から認証が必要なＵＲＬをホスト３１が最初に受信したときに一意のセションＩＤ（図示のように現時刻の年月日時分秒ミリ秒で決まる一意のセションＩＤ）を付加して当該セションテーブル３５のセションＩＤの欄にセットして登録および現時刻に認証有効時間を加算して求めた認証満了時間をセションテーブル３５の当該認証満了時間の欄にセットするものである。そして、セションＩＤをｈｔｍｌ文書に不可視に埋め込んでホスト３１とブラウザ２２との間で任意のＷＷＷサーバ１１を経由して授受し、認証満了時間を経過するまでセションＩＤを有効なものとして扱い、ホスト３１がデータをブラウザ２２に送信したりなどするようにしている。
【００５２】また、セションテーブル３５中のパトロール時間は、当該セションテーブル３５中のエントリ中の認証満了時間を経過して不要なものがあるか否かをパトロールする時間間隔であって、無効なものは削除してメモリ容量を削減するためのものである。また、タイマ監視時間は、各種タイマを監視する時間を設定するものである。
【００５３】尚、セションテーブル３５中のＩＤ、パスワードは、図示外のオフラインでユーザＩＤおよびパスワードを登録したマスタＤＢに登録されたユーザＩＤ、パスワードのコピーである。
【００５４】図５は、本発明のＩＤ／パスワード入力画面例を示す。これは、既述した図２のＳ２０でブラウザ２２の画面上に表示したＩＤ／パスワードの入力画面例であって、図示のように、ユーザＩＤ、パスワードを入力する領域を表示したものである。これらユーザＩＤおよびパスワードの入力領域に入力してＳＴＡＲＴボタンを押下すると、既述した図２のＳ２２によって暗号化してＷＷＷサーバ１１に送出する。
【００５５】図６は、本発明のＩＤ／パスワード認証フローチャートを示す。図６において、Ｓ５１は、ＩＤ／パスワードがマスタＤＢに登録済か判別する。ＹＥＳの場合には、Ｓ５２で認証ＯＫと判別する。ＮＯの場合には、図５のＩＤ／パスワード入力画面上で入力されたＷＷＷサーバ１１を経由してホスト３１に通知されたＩＤ、パスワードがマスタＤＢに登録されいないと判明したので、Ｓ５３で認証ＮＧと決定する。
【００５６】図７は、本発明の認証範囲の判定フローチャートを示す。これは、既述した図３のセキュリティテーブル３４に登録されたＴＹＰＥをもとに認証範囲を判定するフローチャートである。
【００５７】図７において、Ｓ６１は、ＵＲＬで指定された図３のセキュリティテーブル３４のＴＹＰＥの欄の値（００、０１、ＢＳ、ＰＵＢ）のいずれかを判別する。Ｓ６２は、ＴＹＰＥの欄の値（００、０１、ＢＳ、ＰＵＢ）によってそれぞれ認証ＯＫ／認証ＮＧの判定を行う。
【００５８】・ＴＹＰＥ＝００の場合には、Ｓ６３で有料サービス資格有か判別し、ＹＥＳのときにＳ６４で認証ＯＫと判定され、ＮＯのときにＳ６５で認証ＮＧと判定される。
【００５９】・ＴＹＰＥ＝０１の場合には、Ｓ６６で無料サービス資格有か判別し、ＹＥＳのときにＳ６７で認証ＯＫと判定され、ＮＯのときにＳ６８で認証ＮＧと判定される。
【００６０】・ＴＹＰＥ＝ＢＳの場合には、Ｓ６９で認証ＯＫと判定される。
・ＴＹＰＥ＝ＰＵＢの場合には、Ｓ７０で認証ＯＫと判定される。
図８は、本発明のＵＲＬ／ｈｔｍｌ文書例を示す。
【００６１】図８の（ａ）は、ＵＲＬの例を示す。ここでは、
URLは、http://www.fujitsu.co.jp
html文書は、当該html文書中に図示の
・HREF:URLデータ
を埋め込んだものである。
【００６２】図８の（ｂ）は、ＵＲＬ（セションＩＤ付加）の例を示す。ここでは、
URL(セションID付加)は、http://www.fujitsu.co.jp？END=yymmddhhmmssxxx
html文書は、当該html文書中に図示の
・HREF:URL(セションID)データ
を埋め込んだもの(不可視に埋め込んだもの)である。このＵＲＬ（セションＩＤ付加）をそのままブラウザ２２に送出すると、明示的に表示されてしまい、セションＩＤが見えてしまうので、このままではブラウザ２２に送出しない。
【００６３】図８の（ｃ）は、ＵＲＬ（ｃｇｉ付加）の例を示す。ここでは、
URL(cgi付加)は、http://www.fujitsu.co.jp/xxxx.cgi
html文書は、当該html文書中に図示の
・HREF:URL(セションID)データ
を埋め込んだもの(不可視に埋め込んだもの)である。こ

のＵＲＬ（ｃｇｉ付加）をブラウザ２２に送出しても、明示的に「・・・ｘｘｘｘ．ｃｇｉ」が表示されるので、セションＩＤ「yymmddhhmmssxxx」が明示的に表示されることはなく、秘密に保持することが可能となる。

【００６４】

【発明の効果】以上説明したように、本発明によれば、複数のいずれかのＷＷＷサーバから通知されたブラウザからのＨＴＭＬ文書を解析し、セションＩＤが付加されていなかったときにユーザ情報の入力要求をＷＷＷサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセションＩＤを生成し、ふたたびＷＷＷサーバを介してセションＩＤの埋め込んだＨＴＭＬ文書をブラウザに送信すると共に、有効時間情報を管理し、有効時間情報の範囲内のときに認証を許す構成を採用しているため、利用者が一度認証すれば認証有効時間内は付与された一意の不可視のセションＩＤをもとに複数ページや異なる複数のＷＷＷサーバに渡ってアクセスすることができる。このように不可視のセションＩＤによって複数のＷＷＷサーバに跨がったセション管理を実現することが可能となった。

【図面の簡単な説明】

【図１】本発明のシステム構成図である。

＊【図２】本発明の動作説明図である。

【図３】本発明のセキュリティテーブル例である。

【図４】本発明のセションテーブル例である。

【図５】本発明のＩＤ／パスワード入力画面例である。

【図６】本発明のＩＤ／パスワード認証フローチャートである。

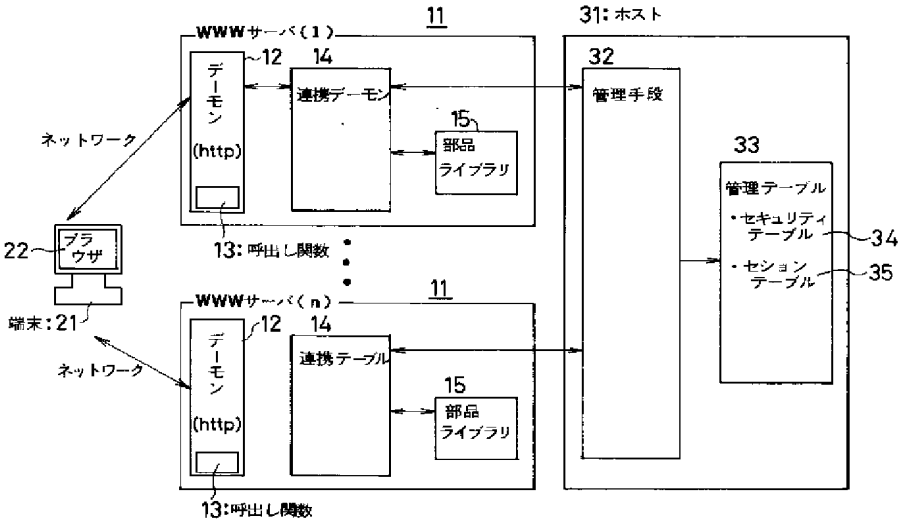
【図７】本発明の認証範囲の判定フローチャートである。

【図８】本発明のＵＲＬ／ｈｔｍｌ文書例である。

【符号の説明】

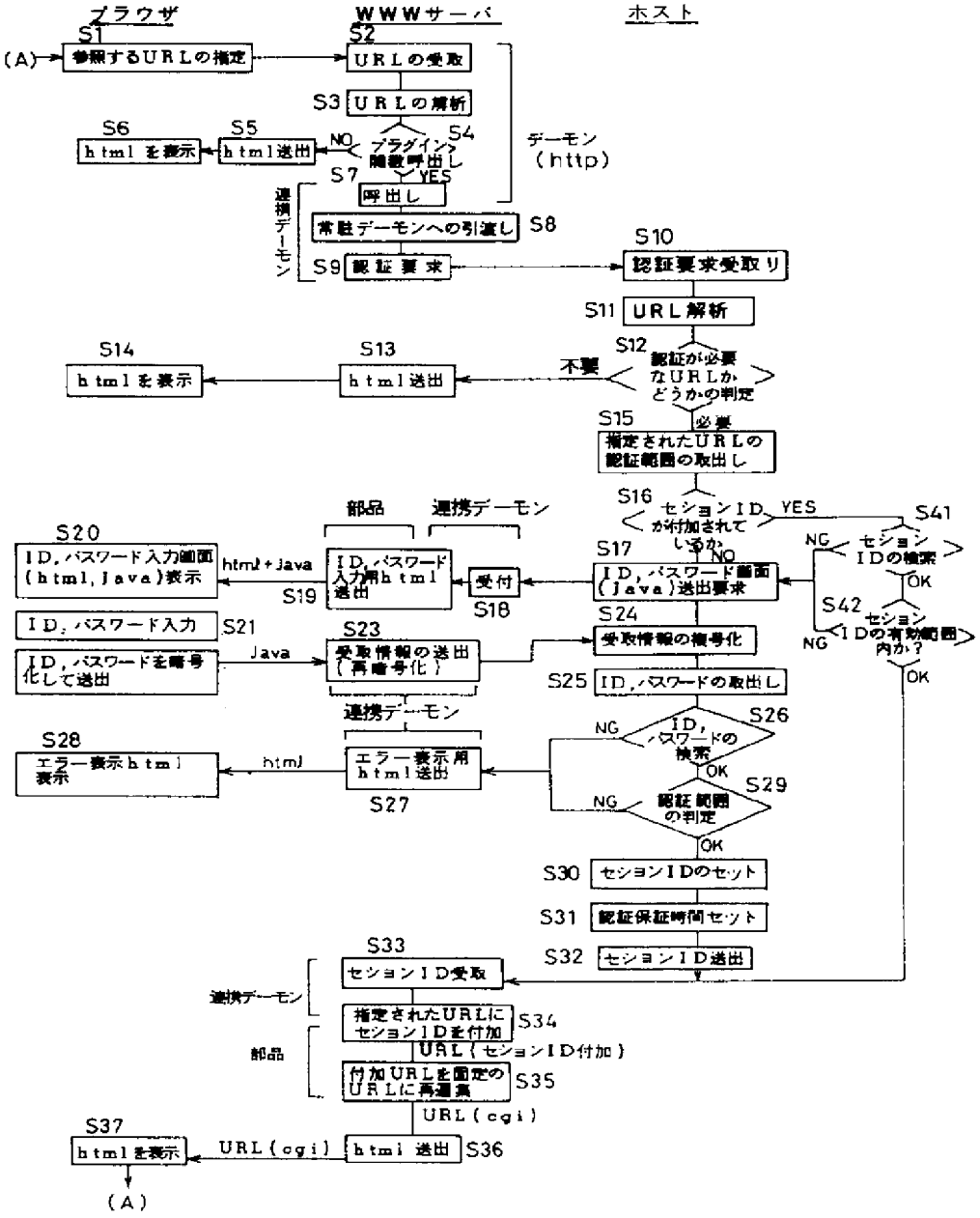
１１：ＷＷＷサーバ
１２：デーモン（ｈｔｔｐ）
１３：呼出し関数
１４：連携デーモン
１５：部品ライブラリ
２１：端末
２２：ブラウザ
３１：ホスト
３２：管理手段
３３：管理テーブル
３４：セキュリティテーブル
３５：セションテーブル

【図１】



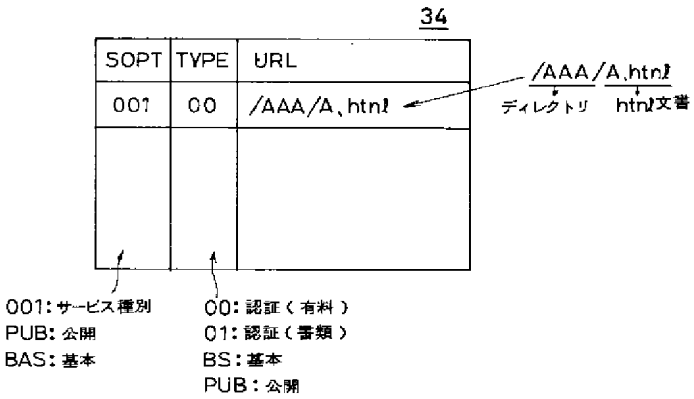
【図２】

本発明の動作説明図



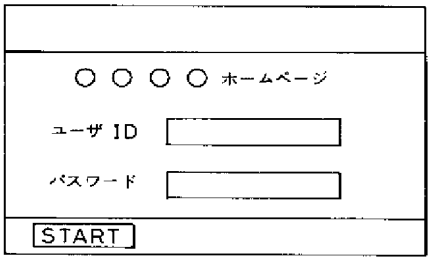
【図３】

本発明のセキュティテーブル例



【図５】

本発明のＩＤ／パスワード入力画面例



【図４】

本発明のセションテーブル例

35

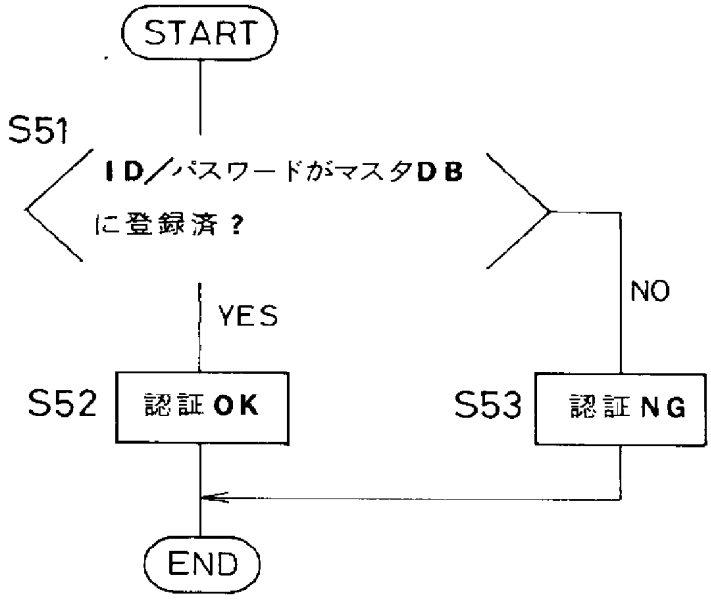
セションid	ID	パスワード	認証有効時間 A+r	パトロール時間 P+r	タイマ監視間隔 Tsup	認証満了時間 Tau+h
yymmddhhmmssxxx	A	XXX	003000	001000	001000	013000

マスタDBのコピー

セションID　yy mm dd hh mm ss xxx
年 月 日 時 分 秒 ミリ秒

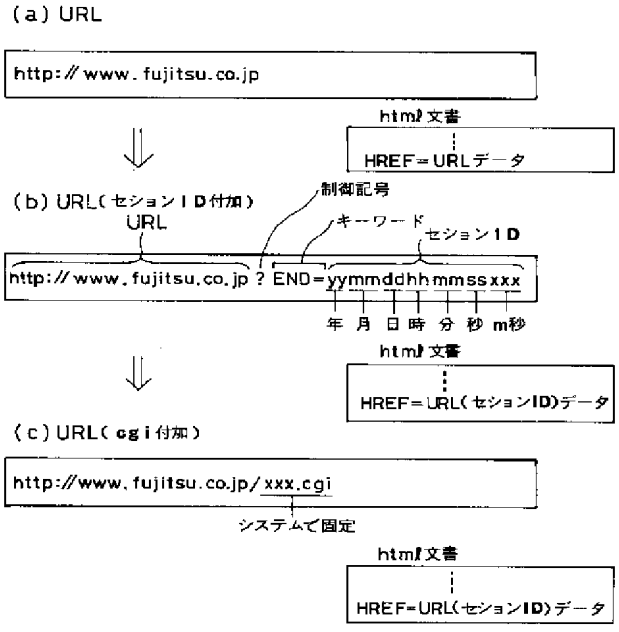
【図６】

本発明のＩＤ／パスワード認証フローチャート



【図８】

本発明のＵＲＬ／ｈｔｍｌ文書例



【図７】

本発明の認証範囲の判定フローチャート